What is claimed is:

1. A digital work protection system including a recording apparatus and a plurality of reproduction apparatuses, the recording apparatus being operable to encrypt a content and write the encrypted content onto a recording medium, and the plurality of reproduction apparatuses each being operable to attempt to decrypt the encrypted content recorded on the recording medium, wherein

one or more of the plurality of reproduction apparatuses are revoked,

the recording medium has (i) a read-only unrewritable area in which a medium inherent number inherent to the recording medium is prestored and (ii) a rewritable area to and from which data can be written and read, and

the recording apparatus includes:

a storing unit that stores therein a piece of media key data including a plurality of encrypted media keys generated by (i) for each of unrevoked reproduction apparatuses, encrypting a media key using a device key of the unrevoked reproduction apparatus respectively, and (ii) for each of the revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively;

a reading unit operable to read the medium inherent number from the unrewritable area of the recording medium;

a generating unit operable to generate an encryption key based on the read medium inherent number and the media key;

an encrypting unit operable to encrypt the content being a piece of digital data, based on the generated encryption key, so as to generate the encrypted content;

a reading unit operable to read the piece of media key data from the storing unit; and

a writing unit operable to write the read piece of media key data and the generated encrypted content into the rewritable area of the recording medium, and

each of the reproduction apparatuses includes:

a reading unit operable to read one encrypted media key that corresponds to the reproduction apparatus, from the piece of media key data recorded in the rewritable area of the recording medium;

a decrypting unit operable to decrypt the read encrypted media key using the device key of the reproduction apparatus, so as to generate a decryption media key;

a controlling unit operable to judge whether the generated decryption media key is the detection information or not, to prohibit the encrypted content from being decrypted when

having judged in the affirmative, and to permit the encrypted content to be decrypted when having judged in the negative; and

a decrypting unit operable to, when the encrypted content is permitted to be decrypted, read the encrypted content from the recording medium and decrypt the read encrypted content based on the generated decryption media key, so as to generate a decrypted content.

2. A recording apparatus that is operable to encrypt a content and write the encrypted content onto a first recording medium and is used in a digital work protection system which includes the recording apparatus and a plurality of reproduction apparatuses each being operable to attempt to decrypt the encrypted content recorded on the first recording medium, wherein

one or more of the plurality of reproduction apparatuses are revoked,

the first recording medium has (i) a read-only unrewritable area in which a medium inherent number inherent to the first recording medium is prestored and (ii) a rewritable area to and from which data can be written and read, and

the recording apparatus includes:

a storing unit that stores therein a first piece of media key data including a plurality of encrypted media keys generated by (i) for each of unrevoked reproduction apparatuses,

encrypting a media key using a device key of the unrevoked reproduction apparatus respectively, and (ii) for each of the revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively;

a first reading unit operable to read the medium inherent number from the unrewritable area;

a generating unit operable to generate an encryption key based on the read medium inherent number and the media key;

an encrypting unit operable to encrypt the content being a piece of digital data, based on the generated encryption key, so as to generate the encrypted content;

a second reading unit operable to read the first piece of media key data from the storing unit; and

a writing unit operable to write the read first piece of media key data and the generated encrypted content into the rewritable area.

3. The recording apparatus of Claim 2, wherein

a second recording medium stores therein a second piece of media key data including another set of encrypted media keys generated by (i) for each of unrevoked reproduction apparatuses, encrypting the media key using a device key of the unrevoked reproduction apparatus respectively, and (ii) for each of revoked

reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively, and

the recording apparatus further includes:

a comparing unit operable to compare the second piece of media key data recorded on the second recording medium with the first piece of media key data stored in the storing unit so as to judge which is newer; and

an updating unit operable to, when the second piece of media key data has been judged newer, read the second piece of media key data from the second recording medium and overwrite the first piece of media key data stored in the storing unit with the second piece of media key data, and

the second reading unit reads the second piece of media key data from the storing unit, instead of the first piece of media key data, and

the writing unit writes the second piece of media key data, instead of the first piece of media key data, into the rewritable area.

4. The recording apparatus of Claim 3, wherein

the first piece of media key data stored in the storing unit includes a first piece of version information indicating a generation of the first piece of media key data,

the second piece of media key data recorded on the second recording medium includes a second piece of version information indicating a generation of the second piece of media key data, and

the comparing unit judges which one of the first piece of media key data and the second piece of media key data is newer by comparing the first piece of version information with the second piece of version information.

5. The recording apparatus of Claim 3, wherein

the first piece of media key data stored in the storing unit includes a first piece of date and time information indicating a date and time at which the first piece of media key data has been generated,

the second piece of media key data recorded on the second recording medium includes a second piece of data and time information indicating a date and time at which the second piece of media key data has been generated, and

the comparing unit judges which one of the first piece of media key data and the second piece of media key data is newer by comparing the first piece of date and time information with the second piece of date and time information.

6. The recording apparatus of Claim 2, wherein

the storing unit further stores therein a piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked,

the recording apparatus further includes a signature generating unit operable to use a digital signature function on the piece of revocation data, so as to generate a piece of verification information, and

the writing unit further writes the generated piece of verification information into the rewritable area of the first recording medium.

7. The recording apparatus of Claim 6, wherein

the signature generating unit uses a digital signature with appendix on the piece of revocation data to generate a piece of signature data, so as to generate the piece of verification information from the generated piece of signature data and the piece of revocation data, and

the writing unit writes the piece of verification information.

8. The recording apparatus of Claim 6, wherein

the signature generating unit uses a digital signature with message recovery on the piece of revocation data to generate

the piece of verification information.

9. The recording apparatus of Claim 6, wherein

the storing unit further stores therein a secret key and a public key certificate of the recording apparatus,

the signature generating unit uses the digital signature function using the stored secret key,

the second reading unit further reads the public key certificate from the storing unit, and

the writing unit writes the read public key certificate into the rewritable area of the first recording medium.

10. The recording apparatus of Claim 2, wherein

the storing unit further stores therein a public key certificate of the recording apparatus,

the second reading unit reads the public key certificate from the storing unit, and

the writing unit writes the read public key certificate into the rewritable area of the first recording medium.

11. The recording apparatus of Claim 2, wherein

the storing unit further stores therein a piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction

apparatuses are revoked,

the recording apparatus further includes a signature generating unit operable to use a digital signature function on the piece of revocation data so as to generate a piece of verification information, and

the writing unit further writes the generated piece of verification information onto the second recording medium.

12. The recording apparatus of Claim 2, wherein

the storing unit further stores therein a piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked,

the second reading unit further reads the piece of revocation data from the storing unit, and

the writing unit writes the read piece of revocation data onto the second recording medium.

13. The recording apparatus of Claim 2, wherein

the storing unit further stores therein a public key certificate of the recording apparatus,

the second reading unit further reads the public key certificate from the storing unit, and

the writing unit writes the read public key certificate

onto the second recording medium.

14. The recording apparatus of Claim 2, wherein

the storing unit further stores therein an apparatus identifier that identifies the recording apparatus,

the recording apparatus further includes an embedding unit operable to read the apparatus identifier and embed the read apparatus identifier into the content as an electronic watermark, and

the encrypting unit encrypts the content into which the apparatus identifier is embedded.

15. The recording apparatus of Claim 2, wherein

the first piece of media key data stored in the storing unit further includes a first data identifier that identifies the first piece of media key data,

the writing unit (i) writes the first data identifier and the encrypted content into the rewritable area of the first recording medium in such a manner that the first data identifier and the encrypted content are in correspondence with each other, and (ii) writes the first piece of media key data including the first data identifier into the rewritable area.

16. The recording apparatus of Claim 15, wherein

the first recording medium further stores therein a second piece of media key data including another set of encrypted media keys generated by (i) for each of unrevoked reproduction apparatuses, encrypting a media key using a device key of the unrevoked reproduction apparatus respectively, and (ii) for each of revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively,

the second piece of media key data includes a second data identifier that identifies the second piece of media key data, and

the recording apparatus further includes an assigning unit operable to assign the first data identifier, which is different from the second data identifier, to the first piece of media key data stored in the storing unit.

17. The recording apparatus of Claim 15, further including:

a comparing unit operable to compare the first piece of media key data stored in the storing unit with a second piece of media key data recorded on the second recording medium so as to judge which is newer; and

an assigning unit operable to assign the first data identifier to the first piece of media key data when the first piece of media key data has been judged newer.

18. The recording apparatus of Claim 17, wherein

the first piece of media key data stored in the storing unit includes a first piece of date and time information indicating a date and time at which the first piece of media key data has been generated,

a second piece of media key data stored in the first recording medium includes a second piece of data and time information indicating a date and time at which the second piece of media key data has been generated, and

the comparing unit judges which one of the first piece of media key data and the second piece of media key data is newer by comparing the first piece of date and time information with the second piece of date and time information.

19. A reproduction apparatus included in a digital work protection system made up of at least a plurality of reproduction apparatuses and a recording apparatus operable to encrypt a content and write the encrypted content onto a first recording medium, the plurality of reproduction apparatuses each being operable to attempt to decrypt the encrypted content recorded on the first recording medium; wherein

one or more of the plurality of reproduction apparatuses are revoked,

the first recording medium has (i) a read-only

unrewritable area in which a medium inherent number inherent to the first recording medium is prestored and (ii) a rewritable area to and from which data can be written and read,

the recording apparatus stores therein a piece of media key data including a plurality of encrypted media keys generated by (i) for each of unrevoked reproduction apparatuses, encrypting a media key using a device key of the unrevoked reproduction apparatus respectively, and (ii) for each of the revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively,

the recording apparatus (i) reads the medium inherent number from the unrewritable area of the first recording medium (ii) generates an encryption key based on the read medium-inherent number and the media key, (iii) encrypts the content being a piece of digital data based on the generated encryption key to generate the encrypted content, (iv) reads the piece of media key data from the storing unit, and (v) writes the read piece of media key data and the generated encrypted content into the rewritable area of the first recording medium, and

the reproduction apparatus includes:

a reading unit operable to read one encrypted media key that corresponds to the reproduction apparatus, from the piece of media key data recorded in the rewritable area;

a first decrypting unit operable to decrypt the read encrypted media key using the device key of the reproduction apparatus, so as to generate a decryption media key;

a controlling unit operable to judge whether the generated decryption media key is the detection information or not, to prohibit the encrypted content from being decrypted when having judged in the affirmative, and to permit the encrypted content to be decrypted when having judged in the negative; and

a second decrypting unit operable to, when the encrypted content is permitted to be decrypted, read the encrypted content from the first recording medium and decrypt the read encrypted content based on the generated decryption media key, so as to generate a decrypted content.

20. The reproduction apparatus of Claim 19, wherein

the recording apparatus further stores therein a piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked, uses a digital signature function on the piece of revocation data to generate a piece of verification information, and writes the generated piece of verification information into the rewritable area of the first recording medium,

the reading unit further reads the piece of verification

information recorded in the rewritable area,

the reproduction apparatus further includes a verifying unit operable to implement signature verification based on the read piece of verification information and output a verification result indicating either a verification success or a verification failure, and

the controlling unit further prohibits the encrypted content from being decrypted when the verification result indicates a verification failure, and permits the encrypted content to be decrypted when the verification result indicates a verification success.

21. The reproduction apparatus of Claim 20, wherein

the recording apparatus (i) uses a digital signature with appendix on the piece of revocation data to generate a piece of signature data, (ii) generates the piece of verification information from the generated piece of signature data and the piece of revocation data, (iii) writes the generated piece of verification information, and

the verifying unit implements the signature verification based on the piece of signature data included in the piece of verification information.

22. The reproduction apparatus of Claim 20, wherein

the recording apparatus uses a digital signature with message recovery on the piece of revocation data to generate the piece of verification information, and

the verifying unit generates, when the verification result indicates a verification success, the piece of revocation data from the piece of verification information.

23. The reproduction apparatus of Claim 20, wherein

the recording apparatus further stores therein a secret key and a public key certificate of the recording apparatus,

the recording apparatus (i) uses the digital signature function using the stored secret key, (ii) reads the public key certificate, and (iii) writes the read public key certificate into the rewritable area of the first recording medium, and

the verifying unit reads the public key certificate from the first recording medium, extracts a public key from the read public key certificate, and implements the signature verification using the extracted public key.

24. The reproduction apparatus of Claim 20, wherein

the recording apparatus stores therein the piece of revocation data, uses a digital signature function on the piece of revocation data to further generate another piece of verification information, and writes the generated piece of

verification information onto a second recording medium,

the reading unit reads the other piece of verification information from the second recording medium instead of from the first recording medium, and

the verifying unit implements the signature verification based on the other piece of verification information read from the second recording medium.

25. The reproduction apparatus of Claim 19, wherein

the recording apparatus further stores therein a public key certificate of the recording apparatus, reads the public key certificate, and writes the read public key certificate into the rewritable area of the first recording medium,

the reproduction apparatus further includes:

a storing unit that stores therein a first piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked;

a certificate reading unit operable to read the public key certificate from the first recording medium; and

a public key verifying unit operable to check whether a public key included in the read public key certificate is revoked according to the first piece of verification data, and

the controlling unit further prohibits the encrypted content from being decrypted when the public key is revoked, and permits the encrypted content to be decrypted when the public key is not revoked.

26. The reproduction apparatus of Claim 25, wherein

a second recording medium stores therein a second piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked,

the reproduction apparatus further includes:

a comparing unit operable to compare the second piece of revocation data recorded on the second recording medium with the first piece of revocation data stored in the storing unit so as to judge which is newer; and

an updating unit operable to, when the second piece of revocation data has been judged newer, read the second piece of revocation data from the second recording medium and overwrite the first piece of revocation data in the storing unit with the read second piece of revocation data.

27. The reproduction apparatus of Claim 26, wherein

the comparing unit judges which one of the first piece of revocation data and the second piece of revocation data is

newer by comparing sizes of the first and second pieces of revocation data.

28. The reproduction apparatus of Claim 26, wherein

the comparing unit judges which one of the first piece of revocation data and the second piece of revocation data is newer by comparing numbers of the revoked public keys indicated by the first and second pieces of revocation data.

29. The reproduction apparatus of Claim 26, wherein

the first piece of revocation data stored in the storing unit includes a first piece of version information indicating a generation of the first piece of revocation data,

the second piece of revocation data recorded on the second recording medium includes a second piece of version information indicating a generating of the second piece of revocation data, and

the comparing unit judges which one of the first piece of revocation data and the second piece of revocation data is newer by comparing the first and second pieces of version information.

30. The reproduction apparatus of Claim 26, wherein

the first piece of revocation data stored in the storing

unit includes a first piece of date and time information indicating a date and time at which the first piece of revocation data has been generated,

the second piece of revocation data recorded on the second recording medium includes a second piece of date and time information indicating a date and time at which the second piece of revocation data has been generated, and

the comparing unit judges which one of the first piece of revocation data and the second piece of revocation data is newer by comparing the first and second pieces of date and time information.

31. The reproduction apparatus of Claim 25, wherein

the recording apparatus further stores therein a second piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked,

the recording apparatus reads the second piece of revocation data and writes the read second piece of revocation data onto a second recording medium, and

the public key verifying unit reads the second piece of revocation data, instead of the first piece of revocation data, from the second recording medium, and verifies if the public key is revoked according to the second piece of revocation data.

32. The reproduction apparatus of Claim 25, wherein

the recording apparatus further stores therein a public key certificate of the recording apparatus,

the recording apparatus reads the public key certificate and writes the read public key certificate onto a second recording medium, and

the certificate reading unit reads the public key certificate from the second recording medium instead of from the first recording medium.

33. The reproduction apparatus of Claim 19, further comprising:

a storing unit that stores therein an apparatus identifier that identifies the reproduction apparatus; and

an embedding unit operable to, when the encrypted content is permitted to be decrypted, read the apparatus identifier from the storing unit and embed the read apparatus identifier into the encrypted content as an electronic watermark, and

a writing unit operable to write the encrypted content in which the apparatus identifier is embedded onto the first recording medium.

34. The reproduction apparatus of Claim 19, wherein

the piece of media key data stored in the recording

apparatus further includes a data identifier that identifies the piece of media key data,

the recording apparatus writes the data identifier and the encrypted content into the rewritable area in such a manner that the data identifier and the encrypted content are in correspondence with each other, and writes the piece of media key data including the data identifier into the rewritable area, and

the reproduction apparatus further includes:

a receiving unit operable to receive a specification of the encrypted content recorded on the first recording medium;

a first reading unit operable to read, from the first recording medium, the data identifier that is in correspondence with the encrypted content in the received specification; and

a second reading unit operable to read the piece of media key data including the data identifier from the first recording medium, and

the controlling unit judges whether the encrypted content is prohibited from being decrypted or permitted to be decrypted based on the read piece of media key data.

35. A recording method used by a recording apparatus that is operable to encrypt a content and write the encrypted content onto a recording medium and is included in a digital work

protection system being made up of at least the recording apparatus and a plurality of reproduction apparatuses each being operable to attempt to decrypted the encrypted content, wherein

one or more of the plurality of reproduction apparatuses are revoked,

the recording medium has (i) a read-only unrewritable area in which a medium inherent number inherent to the recording medium is prestored and (ii) a rewritable area to and from which data can be written and read, and

the recording apparatus includes

a storing unit that stores therein a piece of media key data including a plurality of encrypted media keys generated by (i) for each of unrevoked reproduction apparatuses, encrypting a media key using a device key of the unrevoked reproduction apparatus respectively, and (ii) for each of the revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively, and

the recording method includes:

a first reading step of reading the medium inherent number from the unrewritable area of the recording medium;

a generating step of generating an encryption key based on the read medium inherent number and the media key;

an encrypting step of encrypting the content being

a piece of digital data, based on the generated encryption key, so as to generate the encrypted content;

a second reading step of reading the piece of media key data from the storing unit; and

a writing step of writing the read piece of media key data and the generated encrypted content into the rewritable area of the recording medium.

36. A recording-purpose computer program to be used by a recording apparatus that is operable to encrypt a content and write the encrypted content onto a recording medium and is included in a digital work protection system being made up of at least the recording apparatus and a plurality of reproduction apparatuses each being operable to attempt to decrypt the encrypted content, wherein

one or more of the plurality of reproduction apparatuses are revoked,

the recording medium has (i) a read-only unrewritable area in which a medium inherent number inherent to the recording medium is prestored and (ii) a rewritable area to and from which data can be written and read, and

the recording apparatus includes

a storing unit that stores therein a piece of media key data including a plurality of encrypted media keys generated

by (i) for each of unrevoked reproduction apparatuses, encrypting a media key using a device key of the unrevoked reproduction apparatus respectively, and (ii) for each of the revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively, and

the recording-purpose computer program includes:

a first reading step of reading the medium inherent number from the unrewritable area of the recording medium;

a generating step of generating an encryption key based on the read medium inherent number and the media key;

an encrypting step of encrypting the content being a piece of digital data, based on the generated encryption key, so as to generate the encrypted content;

a second reading step of reading the piece of media key data from the storing unit; and

a writing step of writing the read piece of media key data and the generated encrypted content into the rewritable area of the recording medium.

37. The recording-purpose computer program of Claim 36, being recorded on a computer-readable recording medium.

38. A reproduction method to be used by each of reproduction

apparatuses included in a digital work protection system made up of at least the reproduction apparatuses and a recording apparatus operable to encrypt a content and write the encrypted content onto a recording medium, the reproduction apparatuses each being operable to attempt to decrypt the encrypted content, wherein

one or more of the plurality of reproduction apparatuses are revoked,

the recording medium has (i) a read-only unrewritable area in which a medium inherent number inherent to the recording medium is prestored and (ii) a rewritable area to and from which data can be written and read, and

the recording apparatus stores therein a piece of media key data including a plurality of encrypted media keys generated by (i) for each of unrevoked reproduction apparatuses, encrypting a media key using a device key of the unrevoked reproduction apparatus respectively, and (ii) for each of the revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively,

the recording apparatus (i) reads the medium inherent number from the unrewritable area of the recording medium, (ii) generates an encryption key based on the read medium inherent number and the media key, (iii) encrypts the content being a

piece of digital data based on the generated encryption key to generate the encrypted content, (v) reads the piece of media key data from the storing unit, and (vi) writes the read piece of media key data and the generated encrypted content into the rewritable area of the recording medium, and

the reproduction method includes:

a reading step of reading one encrypted media key that corresponds to the reproduction apparatus, from the piece of media key data recorded in the rewritable area of the recording medium;

a first decrypting step of decrypting the read encrypted media key using the device key of the reproduction apparatus, so as to generate a decryption media key;

a controlling step of judging whether the generated decryption media key is the detection information or not, prohibiting the encrypted content from being decrypted when having judged in the affirmative, and permitting the encrypted content to be decrypted when having judged in the negative; and

a second decrypting step of, when the encrypted content is permitted to be decrypted, reading the encrypted content from the recording medium, and decrypting the read encrypted content based on the generated decryption media key, so as to generate a decrypted content.

39. A reproduction-purpose computer program to be used by each of reproduction apparatuses that are included in a digital work protection system made up of at least the reproduction apparatuses and a recording apparatus being operable to encrypt a content and write the encrypted content onto a recording medium, the reproduction apparatuses each being operable to decrypt the encrypted content, wherein

one or more of the plurality of reproduction apparatuses are revoked,

the recording medium has (i) a read-only unrewritable area in which a medium inherent number inherent to the recording medium is prestored and (ii) a rewritable area to and from which data can be written and read, and

the recording apparatus stores therein a piece of media key data including a plurality of encrypted media keys generated by (i) for each of unrevoked reproduction apparatuses, encrypting a media key using a device key of the unrevoked reproduction apparatus respectively, and (ii) for each of the revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively,

the recording apparatus (i) reads the medium inherent number from the unrewritable area of the recording medium, (ii) generates an encryption key based on the read medium inherent

number and the media key, (iii) encrypts the content being a piece of digital data based on the generated encryption key to generate the encrypted content, (v) reads the piece of media key data from the storing unit, and (vi) writes the read piece of media key data and the generated encrypted content into the rewritable area of the recording medium, and

the reproduction-purpose computer program includes:

a reading step of reading one encrypted media key that corresponds to the reproduction apparatus, from the piece of media key data recorded in the rewritable area of the recording medium;

a first decrypting step of decrypting the read encrypted media key using the device key of the reproduction apparatus, so as to generate a decryption media key;

a controlling step of judging whether the generated decryption media key is the detection information or not, prohibiting the encrypted content from being decrypted when having judged in the affirmative, and permitting the encrypted content to be decrypted when having judged in the negative; and

a second decrypting step of, when the encrypted content is permitted to be decrypted, reading the encrypted content from the recording medium, and decrypting the read encrypted content based on the generated decryption media key, so as to generate a decrypted content.

40. The reproduction-purpose computer program of Claim 39, being recorded on a computer-readable recording medium.

41. A computer-readable recording medium that includes (i) a read-only unrewritable area and a rewritable area to and from which data can be written and read, wherein

a medium inherent number inherent to the recording medium is prestored in the unrewritable area,

a piece of media key data and an encrypted content are recorded in the rewritable area,

the piece of media key data includes a plurality of encrypted media keys generated by (i) for each of unrevoked reproduction apparatuses, encrypting a media key using a device key of the unrevoked reproduction apparatus respectively, and (ii) for each of the revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively,

the encrypted content is generated by encrypting a content being a piece of digital data, based on an encryption key, and

the encryption key is generated based on the medium inherent number and the media key recorded in the unrewritable area of the recording medium.

42. A computer-readable recording medium that includes (i)

a read-only unrewritable area and a rewritable area to and from which data can be written and read, wherein

a medium inherent number inherent to the recording medium is prestored in the unrewritable area,

a piece of media key data and an encrypted content are recorded in the rewritable area,

the piece of media key data includes a plurality of encrypted media keys generated by (i) for each of unrevoked reproduction apparatuses, encrypting a media key using a device key of the unrevoked reproduction apparatus respectively, and (ii) for each of the revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively, and further includes a data identifier that identifies the piece of media key data,

the encrypted content is generated by encrypting a content being a piece of digital data based on an encryption key, and includes the data identifier, and

the encryption key is generated based on the medium inherent number and the media key recorded in the unrewritable area of the recording medium.